

# Ancilla-Driven Universal Blind Quantum Computation

Takahiro Sueki,<sup>1</sup> Takeshi Koshihara,<sup>1</sup> and Tomoyuki Morimae<sup>2</sup>

<sup>1</sup>*Division of Mathematics Electronics and Informatics,  
Graduate School of Science and Engineering, Saitama University,  
255 Shimo-Okubo, Sakura, Saitama 338-8570, Japan*

<sup>2</sup>*Department of Physics, Imperial College London, London SW7 2AZ, United Kingdom*

Blind quantum computation is a new quantum secure protocol, which enables Alice who does not have enough quantum technology to delegate her computation to Bob who has a fully-fledged quantum power without revealing her input, output and algorithm. So far, blind quantum computation has been considered only for the circuit model and the measurement-based model. Here we consider the possibility and the limitation of blind quantum computation in the ancilla-driven model, which is a hybrid of the circuit and the measurement-based models.

## I. INTRODUCTION

Traditionally, quantum computation has been studied in the circuit model [1], where the quantum register which stores quantum information consists of many qubits, and a quantum gate operation is performed by directly accessing one or two qubits in the quantum register. Another canonical model of quantum computation is the one-way model [2] (or more general measurement-based models [3–13]), where the universal quantum computation is performed by adaptive local measurements on a highly entangled resource state. Recently, a mixture of those two models, which is called the ancilla-driven quantum computation, was proposed in [14, 15]. In this model, the quantum register is a set of many qubits like the circuit model, whereas a quantum gate operation is, like the one-way model, performed by adaptive local measurements: one or two register qubits are coupled to a single mobile ancilla, and the ancilla is measured after establishing the interaction between the ancilla and register qubit(s). The backaction of this measurement provides the desired gate operation, such as a single qubit rotation or an entangling two-qubit operation, on register qubit(s). In the ancilla-driven model, the universal quantum computation is performed with only a single type of interaction ( $CZ$  or  $SWAP + CZ$ ) between the ancilla and register qubit(s). It is a great advantage for experiments, since in many experimental setups, implementing various different types of interactions at the same time is very difficult (such as the solid-based quantum computation). Furthermore, the roles of the register and the information carrier are clearly separated, and no direct action on the register is required. Therefore, it is also useful for experimental systems where measurements destroy quantum states, such as photonic systems. In short, this model is a natural theoretical model of the “hybrid quantum computer” where the flying ancilla mediates interactions between static qubits (such as the chip-based quantum computation [16, 17] or the hybrid system of matter and optical elements [18, 19]).

In a future when a scalable quantum computer is realized, the quantum computation should be done in the “cloud” style, since only limited number of people

would have enough money and technology to create and maintain quantum computers. Blind quantum computation [20–29] ensures the privacy of the client in such a cloud quantum computing. In protocols of blind quantum computation, Alice, the client, does not have enough quantum technology. On the other hand, Bob, the server, has a fully-fledged quantum power. Alice asks Bob to perform her computation on his quantum computer in such a way that Bob cannot learn anything about her input, output, and algorithm. Blind quantum computation was initially considered by using the circuit model [20–22]. However, in this case, Alice needs a quantum memory. Recent new ideas of blind quantum computation which use measurement-based models have succeeded to exempt Alice from a quantum memory [23–29].

In terms of the computational power, measurement-based models do not offer any advantage over the circuit model, since the circuit model can be simulated by measurement-based models and vice versa. However, measurement-based models have provided new points of view for studying quantum computation, and in fact such new viewpoints have enabled plenty of successes which have never been done in the circuit model, such as the high-threshold fault-tolerancy [10–12, 30–36], clarifying roles of entanglement played in quantum computation [3, 37–40], and relations to condensed-matter physics [3–7, 13, 41–44]. Therefore it is important to explore the possibility of blind quantum computation on other models than the circuit model and measurement-based models.

## II. PRELIMINARIES

We first define several notations for the bases and for the basic transformations as follows.

$$\begin{aligned} |+\theta, \varphi\rangle &= \cos\left(\frac{\theta}{2}\right)|0\rangle + e^{i\varphi}\sin\left(\frac{\theta}{2}\right)|1\rangle, \\ |-\theta, \varphi\rangle &= \sin\left(\frac{\theta}{2}\right)|0\rangle - e^{i\varphi}\cos\left(\frac{\theta}{2}\right)|1\rangle, \\ R_x(\theta) &= e^{-\frac{i\theta X}{2}} = \begin{pmatrix} \cos\frac{\theta}{2} & -i\sin\frac{\theta}{2} \\ -i\sin\frac{\theta}{2} & \cos\frac{\theta}{2} \end{pmatrix}, \text{ and} \\ R_z(\theta) &= e^{-\frac{i\theta Z}{2}} = \begin{pmatrix} 1 & 0 \\ 0 & e^{i\theta} \end{pmatrix}. \end{aligned}$$

We conventionally use the notations  $\{|\pm\rangle\}$  and  $\{|0\rangle, |1\rangle\}$  to denote the bases along  $X$  and  $Z$  axes in Bloch sphere, respectively. Measurement outcome is represented by  $s \in \{0, 1\}$ , associated with  $\pm$ . We denote by  $s_i$  the  $i$ th measurement outcome.

### III. ANCILLA-DRIVEN QUANTUM COMPUTATION

We review the ancilla-driven quantum computation (ADQC) model proposed in [15]. ADQC is performed with (a single or a few) entangle operator(s)  $\tilde{E}_{as}$ . As in Fig.1-(a),  $\tilde{E}_{as}$  can be decomposed into  $\tilde{E}_{as} = (W_s \otimes W'_a)D_{as}(V_s \otimes V'_a)$ , where  $V_s, V'_a, W_s$  and  $W'_a$  are local unitaries and  $D_{as}$  is a non-local unitary, by the Cartan decomposition [45]. Fig.1-(a) can be rewritten to Fig.1-(b) by applying  $V'_a$  to the initial ancilla state  $|+\rangle_a$  and  $W'_a$  to the measurement basis  $\{|0\rangle, |1\rangle\}$ .  $D_{as}$  is described as

$$D_{as} = e^{-i(\alpha_x X_a \otimes X_s + \alpha_y Y_a \otimes Y_s + \alpha_z Z_a \otimes Z_s)}$$

by using non-symmetric parameters  $0 \leq \alpha_x, \alpha_y, \alpha_z \leq \frac{\pi}{4}$  due to the Weyl chamber [46].

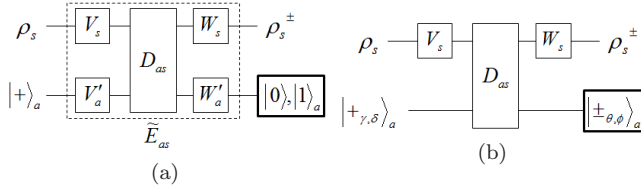


FIG. 1. ADQC model. Rectangle boxes with bold line represents measurements and the inside represents bases for the measurements.

For universal quantum computation, we should choose all the parameters appropriately. To this end, Anders *et al.* in [15] derive sufficient conditions for (i) Unitarity, (ii) *One-step* Correctable Branching, (iii) Standardization and (iv) Universality. Especially, we will discuss about *One-step* Correctable Branching, which states that the generalized Pauli correction (according to the measurement outcome) after “one” execution of the operation in Fig.1-(b) enables the Kraus operator acting on the system deterministic. In order to fulfill these conditions, it is shown that the entangle operator  $\tilde{E}_{as}$  must be locally equivalent to either SWAP+CZ or CZ.

### IV. ANCILLA-DRIVEN UNIVERSAL BLIND QUANTUM COMPUTATION

SWAP+CZ type can be considered as an extension of one-way quantum computation, so we can actually perform universal blind computation as in [23]. Therefore we only investigate universal blind computation of CZ type. Requiring the above four conditions is too strong for the blind ADQC model of CZ type. Actually, we have the following.

**Theorem 1.** *ADQC of CZ type satisfying all the conditions from (i) to (iv) cannot be universal blind quantum computation (in the sense of [23]).*

*Proof.* The system Kraus operator for  $\tilde{E}_{as}$  is specified as an excepted local unitaries  $K_s^\pm = {}_a\langle \pm_{\theta, \varphi} | D_{as} | +_{\gamma, \delta} \rangle_a$ . As in [15], conditions for Unitarity and One-step Correctable Branching require that the parameters for ancilla satisfy  $\sin \theta \cos \gamma \sin \phi = \cos \theta \sin \gamma \sin \delta$  and Kraus operator  $K_s^\pm = f_\pm I + i(-1)^{n_\pm} g_\pm X_s$ , where  $n_\pm$  are integers that differ in the parity. Each coefficient is rewritten as follows:

$$f_\pm = \frac{\cos \alpha_x}{\sqrt{2}} \sqrt{1 \pm \cos \gamma \cos \theta \pm \sin \gamma \sin \theta \cos(\delta - \phi)}$$

$$g_\pm = \frac{\sin \alpha_x}{\sqrt{2}} \sqrt{1 \mp \cos \gamma \cos \theta \pm \sin \gamma \sin \theta \cos(\delta + \phi)}$$

Therefore, all the conditions from (i) to (iv) imply that admissible parameters of ancilla are classified into the following four cases.

initial state	measurement basis	Kraus operator
$\gamma = 0$	$\theta = 0$	$K_s^\pm = X^s I$
$\gamma = 0$	$\theta = \text{any}$	$K_s^\pm = X^s R_x(\theta)$
$\gamma = \frac{\pi}{2}$	$\theta = 0$	$K_s^\pm = X^s X$
$\gamma, \delta = \text{any}$	$\theta = \frac{\pi}{2}, \phi = 0$	$K_s^\pm = X^s X$

For “universal” blind computation, a rotation operator, e.g.,  $R_x(\theta)$  is necessary. Thus, we have only to consider the second case. In that case, the initial state of the ancilla should be fixed to  $|0\rangle$  since  $\gamma = 0$ . This means that we cannot rotate the initial state to make the computation blind.  $\square$

From the above, we consider to disregard the *One-step* Correctable Branching condition and derive some more admissible parameters of ancilla as follows.

initial state	measurement basis	Kraus operator
$\gamma = \text{any}, \delta = 0$	$\theta = \text{any}, \phi = 0$	$K_s^+ = \cos(\frac{\gamma-\theta}{2})I - i \sin(\frac{\gamma+\theta}{2})X$ $K_s^- = \sin(\frac{\gamma-\theta}{2})I - i \cos(\frac{\gamma+\theta}{2})X$
$\gamma, \delta = \text{any}$	$\theta = \gamma, \phi = \delta$	$K_s^+ = I - i \sin \gamma \cos \delta X$ $K_s^- = (i \sin \delta - \cos \gamma \cos \delta)X$

In addition, we consider to relax *One-step* Correctable Branching to *Multiple-step* and provide a sufficient condition which can make ADQC of CZ type blind.

**Theorem 2** (sufficient condition for the blindness). *In ADQC model, if universal quantum computation satisfies all the following conditions, we can make the computation blind, where Condition 3' is alternative to Condition 3. In the following, rotations are with respect to  $X, Y$  or  $Z$  axes in Bloch sphere.*

1. Rotation  $R(\xi)$  can be simulated with measurement basis parameter  $\xi$ . This unitary can be described as  $WR(\xi)V$  up to Pauli correction, where  $V$  and  $W$  are Clifford operators.

2. Rotation  $R'(\varphi)$  can be simulated with initial state parameter  $\varphi$ . This unitary can be described as  $W'R'((-1)^s\varphi)V'$ , where  $V'$  and  $W'$  are Clifford operators and  $s$  is an outcome of the measurement in this simulation so the unitary is not correctable.
3. With respect to unitaries simulated in Conditions 1 and 2, the following equation holds:  

$$WR(\xi)VW'R'(\varphi)V' = WR(\xi')VW'V' \stackrel{\text{def}}{=} S,$$
where  $\xi' = \xi + (-1)^n\varphi$  and  $n$  is an integer number.
- 3' Clifford operator  $E$  up to Pauli correction can be simulated. With respect to unitaries simulated in Conditions 1 and 2, the following equation holds:  

$$WR(\xi)VEW'R'(\varphi)V' = WR(\xi')VEW'V' \stackrel{\text{def}}{=} S',$$
where  $\xi' = \xi + (-1)^n\varphi$  and  $n$  is an integer number.
- 4 A gate pattern which can perform both  $U \otimes U'$ , tensor product of any one-qubit unitaries  $U$  and  $U'$ , and one kind of two-qubit unitaries is composable by using an unitary  $S$  (or  $S'$ ), an entangle operator or a controlled-Pauli that can be simulated.

*Proof.* We can perform an arbitrary quantum computation by tiling the gate pattern in Condition 4 regularly as in Fig.2. What unitaries the gate pattern performs depends on a parameter  $\xi'$  of each gate in Condition 3 (or 3') composing the gate pattern. When Client chooses a parameter  $\xi'$ , Client sends a measurement basis parameter  $\xi$  such that  $\xi = \xi' - (-1)^n\varphi$ . By choosing an initial state parameter  $\varphi$  randomly,  $\xi$  also looks random to Server. This process is performed similarly to the protocol in [23]. We use the following protocol for the simulation of  $S$  (or  $S'$ ).

1. Client chooses a parameter  $\varphi$  of ancilla randomly and sends the ancilla to Server.
2. Server performs the simulation of  $W'R(\varphi)V'$  with the given ancilla. (The simulation of  $E$  is optional.) Server sends the outcome(s) of the measurement in this simulation to Client.
3. Client decides  $\xi'$  and calculates  $\xi = \xi' - (-1)^n\varphi + r\pi$  with a random bit  $r \in \{0, 1\}$  then sends  $\xi$  to Server.
4. Server performs the simulation of  $WR(\xi)V$  and sends a bit  $b$  as the outcome of the measurement in this simulation to Client.
5. Client inverts the bit value  $b$  if  $r = 1$ .

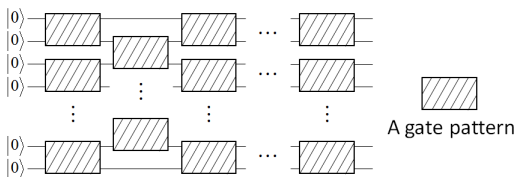


FIG. 2. Universal gate pattern.

In this protocol, each ancilla state is maximally mixed state and each  $\xi$  looks random to Server. Therefore, the information leaked to Server is only the size of the universal gate pattern, that is, the input size and the depth of the computation.  $\square$

For satisfying Conditions 2 and 3 stated in Theorem 2, we have that the Kraus operators are written as

$$K_s^+ = R_x(\gamma) \text{ and } K_s^- = R_x(-\gamma - \pi)$$

if we choose the initial state parameters  $\gamma$  be any value and  $\delta = 0$  and the measurement bases parameters  $\phi, \theta = 0$ . Then, we have the following.

**Theorem 3.** Condition 3 and 4 do not hold simultaneously if we can use only one kind of entangle operators.

*Proof.* From Condition 3 for the blindness, it must hold that  $WR_x(\theta)VW'Rx((-1)^s\varphi)V = WR_x(\theta + (-1)^n\varphi)VW'V$ . These  $V$  and  $W$  are denoted as  $aI + ibX$  or  $aY + bZ$ , up to the global phase, where  $a, b \in \mathbb{R}$ . So, any unitary  $U$  composed of  $WR_x(\theta)VW'Rx((-1)^s\varphi)V$  is described  $U = W\tilde{U}V$  with the kernel  $\tilde{U}$  which moves a quantum state only in one plane of Bloch sphere, parallel to the  $Y$ - $Z$  plane. If  $V$  and  $W$  are determined,  $U$  becomes an unitary which moves a quantum state only in one plane of Bloch sphere so we cannot perform any arbitrarily rotation  $U \otimes U'$  in Condition 4. Therefore we cannot satisfy Conditions 3 and 4 simultaneously.  $\square$

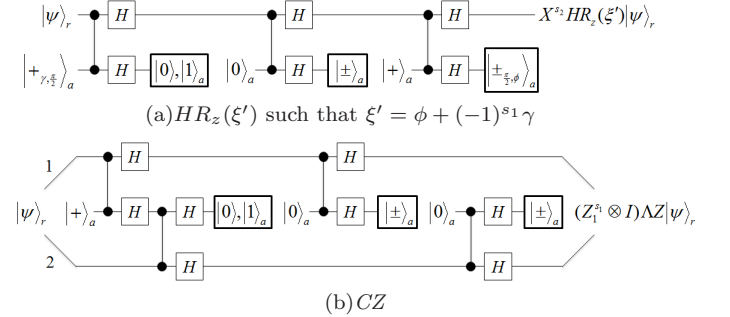


FIG. 3. Simulating  $HR_z(\xi')$  and  $CZ$ .

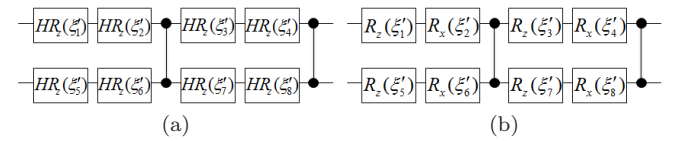


FIG. 4. Gate pattern (a) is for a single entangle operator and (b) for two entangle operators.

**Theorem 4.** Conditions 3' and 4 can hold simultaneously if we use one kind of entangle operators.

*Proof.* It is enough to show a way of simulations and a gate pattern. The simulation in Condition 3 and a controlled-Pauli in Condition 4 are shown in Fig.3. A gate pattern in Condition 4 is shown in Fig.4(a).  $\square$

**Theorem 5.** *Conditions 3 and 4 can hold simultaneously if we use two kinds of entangle operators.*

*Proof.* It is enough to show a way of simulations and a gate pattern. The simulation in Condition 3 is shown in Fig.5 and a gate pattern in Condition 4 is shown in Fig.4(b).  $\square$

**Corollary 1.** *Universal blind computation in ADQC model is possible since we can satisfy the sufficient condition for the blindness.*

## V. CONCLUSION

In this paper, we considered the limitation and possibilities for universal blind computation in ADQC model. First, we proved that if we satisfy all the conditions for

universal quantum computation in [15], we can not perform universal blind computation. Therefore, we relaxed some conditions and derived a sufficient condition for the blindness. Finally, we provided a way of universal blind computation in ADQC model.

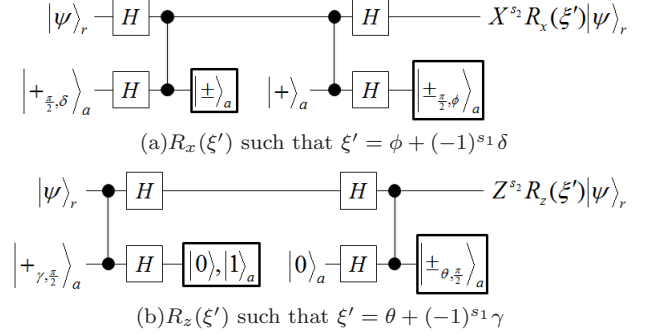


FIG. 5. Simulating  $R_x(\xi')$  and  $R_z(\xi')$ .

- 
- [1] M. Nielsen and I. L. Chuang, *Quantum Computation and Quantum Information*, Cambridge Univ. Press (2000).
  - [2] R. Raussendorf and H. J. Briegel, Phys. Rev. Lett. **86**, 5188 (2001).
  - [3] D. Gross and J. Eisert, Phys. Rev. Lett. **98**, 220503 (2007).
  - [4] G. K. Brennen and A. Miyake, Phys. Rev. Lett. **101**, 010502 (2008).
  - [5] A. Miyake, Phys. Rev. Lett. **105**, 040501 (2010).
  - [6] A. Miyake, Ann. Phys. **326**, 1656 (2011).
  - [7] T. C. Wei, I. Affleck, and R. Raussendorf, Phys. Rev. Lett. **106**, 070501 (2011).
  - [8] J. Cai, A. Miyake, W. Dur, and H. J. Briegel, Phys. Rev. A **82**, 052309 (2010).
  - [9] X. Chen, B. Zeng, Z. Gu, B. Yoshida, and I. L. Chuang, Phys. Rev. Lett. **102**, 220501 (2009).
  - [10] R. Raussendorf, J. Harrington, and K. Goyal, New J. Phys. **9**, 199 (2007).
  - [11] Y. Li, D. E. Browne, L. C. Kwek, R. Raussendorf, and T. C. Wei, Phys. Rev. Lett. **107**, 060501 (2011).
  - [12] K. Fujii and T. Morimae, Phys. Rev. A **85**, 010304(R) (2012).
  - [13] T. Morimae, Phys. Rev. A **85**, 062328 (2012).
  - [14] J. Anders, D. K. L. Oi, E. Kashefi, D. E. Browne and E. Andersson, Phys. Rev. A **82**, 020301(R) (2010).
  - [15] J. Anders, E. Andersson, D. E. Browne, E. Kashefi and D. K. L. Oi, Theor. Comput. Sci. **430**, 51 (2012).
  - [16] R. Ionicioiu, T. P. Spiller, and W. J. Munro, Phys. Rev. A **80**, 012312 (2009).
  - [17] S. J. Devitt, A. G. Fowler, A. M. Stephens, A. D. Green-tree, L. C. L. Hollenberg, W. J. Munro, and K. Nemoto, New J. Phys. **11**, 083032 (2009).
  - [18] T. P. Spiller, K. Nemoto, S. L. Braunstein, W. J. Munro, P. van Loock, and G. J. Milburn, New J. Phys. **8**, 30 (2006).
  - [19] P. van Loock, W. J. Munro, K. Nemoto, T. P. Spiller, T. D. Ladd, S. L. Braunstein, and G. J. Milburn, Phys. Rev. A **78**, 022303 (2008).
  - [20] A. M. Childs, Quant. Inf. Comput. **5**, 456 (2005).
  - [21] P. Arrighi and L. Salvail, Int. J. Quant. Inf. **4**, 883 (2006).
  - [22] D. Aharonov, M. Ben-Or, and E. Eban, Proc. Innov. Comput. Sci. 453, (2010).
  - [23] A. Broadbent, J. Fitzsimons and E. Kashefi, Proc. 50th IEEE Symp. Found. Comput. Sci., 517 (2009).
  - [24] S. Barz, E. Kashefi, A. Broadbent, J. F. Fitzsimons, A. Zeilinger, and P. Walther, Science **335**, 303 (2012).
  - [25] T. Morimae, V. Dunjko, and E. Kashefi, arXiv:1009.3486.
  - [26] V. Dunjko, E. Kashefi, and A. Leverrier, Phys. Rev. Lett. **108**, 200502 (2012).
  - [27] T. Morimae and K. Fujii, Nature Communications **3**, 1036 (2012).
  - [28] T. Morimae and K. Fujii, arXiv:1201.3966.
  - [29] J. F. Fitzsimons and E. Kashefi, arXiv:1203.5217.
  - [30] M. A. Nielsen and C. M. Dawson, Phys. Rev. A **71**, 042323 (2005).
  - [31] P. Aliferis and D. W. Leung, Phys. Rev. A **73**, 032308 (2006).
  - [32] M. Varnava, D. Browne, and T. Rudolph, Phys. Rev. Lett. **97**, 120501 (2006).
  - [33] T. Morimae and K. Fujii, Sci. Rep. **2**, 508 (2012).
  - [34] S. D. Barrett and T. M. Stace, Phys. Rev. Lett. **105**, 200502 (2010).
  - [35] K. Fujii and Y. Tokunaga, Phys. Rev. Lett. **105**, 250503 (2010).
  - [36] Y. Li, S. D. Barrett, T. M. Stace, and S. C. Benjamin, Phys. Rev. Lett. **105**, 250502 (2010).
  - [37] M. Van den Nest, A. Miyake, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **97**, 150504 (2006).
  - [38] T. Morimae, Phys. Rev. A **81**, 060307(R) (2010).
  - [39] D. Gross, et. al. Phys. Rev. Lett. **102**, 190501 (2009).
  - [40] M. Bremner, et. al. Phys. Rev. Lett. **102**, 190502 (2009).
  - [41] F. Verstraete and J. I. Cirac, Phys. Rev. A **70**, 060302(R) (2004).
  - [42] M. Van den Nest, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **98**, 117207 (2007).

- [43] M. Van den Nest, W. Dur, and H. J. Briegel, Phys. Rev. Lett. **100**, 110501 (2008).
- [44] K. Fujii and T. Morimae, Phys. Rev. A **85**, 032338 (2012).
- [45] J. Zhang, J. Vala, S. Sastry, K. Birgitta Whaley, Phys. Rev. A **67**, 042313 (2003)
- [46] R. R. Tucci, quant-ph/0507171.